

Amendment
Serial No. 10/069,118
Attorney Docket No. 020234

REMARKS

Claims 23-63 are pending in the above-identified application. Claim 23 is amended. It is respectfully submitted that this response is fully responsive to the Office Action dated June 16, 2005.

Claims 23, 28, 34, 45 and 53 were objected to because it is unclear to the Examiner "which portion of these claims is preamble and which portion is body of the claim." Applicants respectfully disagree with the Examiner's position. Where the preambles end and the body of the claims start is clear from wording in the claims (e.g., transitional words.) Accordingly, Applicants respectfully request that the Examiner's objection be withdrawn.

Claims 23-63 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Specifically, claims 23, 28, 34, 45 and 53, were rejected because, according to the Examiner, it is unclear what the difference between the content key, decryption key, encryption key, session key and public key is. The Examiner asserted that the terms are being used interchangeably which makes it difficult to identify the scope of the claims. Applicants respectfully disagree with the Examiner's position because, interpreted properly, it is clear that the terms are not being used interchangeably in the claims. Also, the Examiner incorrectly interpreted these claims as including an encryption key and a public key. Whereas, in the there is only a "public encryption key" identified in the above claims. Accordingly, Applicants respectfully request that the Examiner withdraw this rejection.

Amendment
Serial No. 10/069,118
Attorney Docket No. 020234

The Examiner stated that is unclear what the first and the second encryption units do in regards to encrypting the keys and the content as far as the claims go. However, these claim features are clearly defined, for example, on page 3, lines 10-13 of the specification and in the claims. Accordingly, Applicants respectfully request that the Examiner either withdraw this reason for rejection or indicate *why* these claim elements are indefinite.

The Examiner also stated that the difference between the first session key and the second session key is unclear. However, these claim elements are clearly explained, for example, in the specification (e.g., page 3, lines 8-13; page 3-1, lines 6-22) and claims of the application. Accordingly, Applicants respectfully request that the Examiner either withdraw this reason for rejection or indicate *why* these claim elements are indefinite.

Claims 26, 49 and 57 were rejected because it is unclear to the Examiner which key is used to encrypt the session key and where the session key is being encrypted (because the claims recite using the private key to encrypt the session key and then the claim recites using the public key to encrypt the session key.) Claims 31, 37 and 43 were rejected because it is unclear to the Examiner which session key is used to obtain the content key or the decryption key. Claims 33, 35, 44, 46 and 54 were rejected because it is unclear to the Examiner what is meant by authentication key or if the authentication key is being used interchangeably with public private key. Claims 37 and 43 were also rejected because it is not clear to the Examiner what is the difference between the unique decryption key in claim 12 and the second decryption key in claims 15 and 21. Applicants respectfully disagree with the Examiner's position on these claim

Amendment
Serial No. 10/069,118
Attorney Docket No. 020234

rejections. The Examiner has failed to point out *why* these claim elements are indefinite. Also, the specification and claims properly explain the above claim elements.

Claims 23-63 were rejected under 35 U.S.C. 102(e) as being anticipated by *Ginter et al.* U.S. (5,917,912). In rejecting these claims, the Examiner asserted that the reference discloses "a session key generation unit generating a session key updated at every access to obtain said content key with respect to said data storage unit" (col. 219, lines 19-25); and "a first encryption processing unit encrypting said session key using a public encryption key that can be decrypted at said data storage unit and that is unique to said data storage unit, and providing said encrypted session key to said data storage unit" (col. 219, lines 41-47). In view of the following remarks, Applicants disagree with the Examiner's position that all claim elements are anticipated by *Ginter et al.* and respectfully request that the rejection of these claims be withdrawn.

Ginter et al. fails to disclose at least the aforementioned features recited in claims 23, 28, 34, 45, and 53. For example, the *Ginter et al.* teaches that "(Party) A must create the (session) key, prove that A created it, and prove that it is associated with the specific proposed communication... (and) the session key must be protected from disclosure or modification to ensure that an attacker cannot substitute a different value." [col. 219, lines 31-39.] *Ginter et al.* does not teach or disclose that the session key is encrypted. Encrypting said session key makes it is difficult for a third party (unauthorized user) to improperly access distribution data as to content data stored in a memory by a proper user. [p. 3/4, lines 8-12.]

Amendment
Serial No. 10/069,118
Attorney Docket No. 020234

Moreover, *Ginter et al.* does not teach or disclose that the session key is updated at every access to obtain a content key with respect to the data storage unit and that a first encryption processing unit encrypts the session key using a public encryption key that is decryptable at the data storage unit and unique to the data storage unit, and provides the encrypted key to the data storage unit. The first decryption processing unit uses the session key to decrypt the encrypted storage unit. The first decryption processing unit uses the session key to decrypt the encrypted content key obtained from the data storage unit in a form encrypted by the session key. [p. 3, lines 8-13.]

Accordingly, the §102(e) rejection of claims 23, 28, 34, 45 and 53 should be withdrawn. As claims 24-27, 29-33, 35-44, 46-52, and 54-63 depend from independent claims 23, 28, 34, 45 and 53, respectively, these claims should likewise be allowable in view of the above comments by nature of their dependency.

For at least the foregoing reasons, the claimed invention distinguishes over the cited art and defines patentable subject matter. Favorable reconsideration is earnestly solicited.

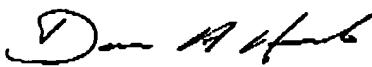
Should the Examiner deem that any further action by applicants would be desirable to place the application in condition for allowance, the Examiner is encouraged to telephone applicants' undersigned attorney.

Amendment
Serial No. 10/069,118
Attorney Docket No. 020234

If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP



Darrin A. Auito
Attorney for Applicants
Registration No. 56,024
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

DAA/meu